FortiToken Mobile 1.0
Administration Guide

FortiToken Mobile 1.0 Administration Guide

Revision 2

December 6, 2013

33-100-186424-20131206

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

FortiToken Mobile Administration

To deploy your FortiToken Mobile tokens for One Time Password use by your end users, you must first install the tokens on your Authentication Server platform; either FortiGate running FortiOS 5.0 or greater, or FortiAuthenticator. After installing the tokens, you can assign them to your end users.

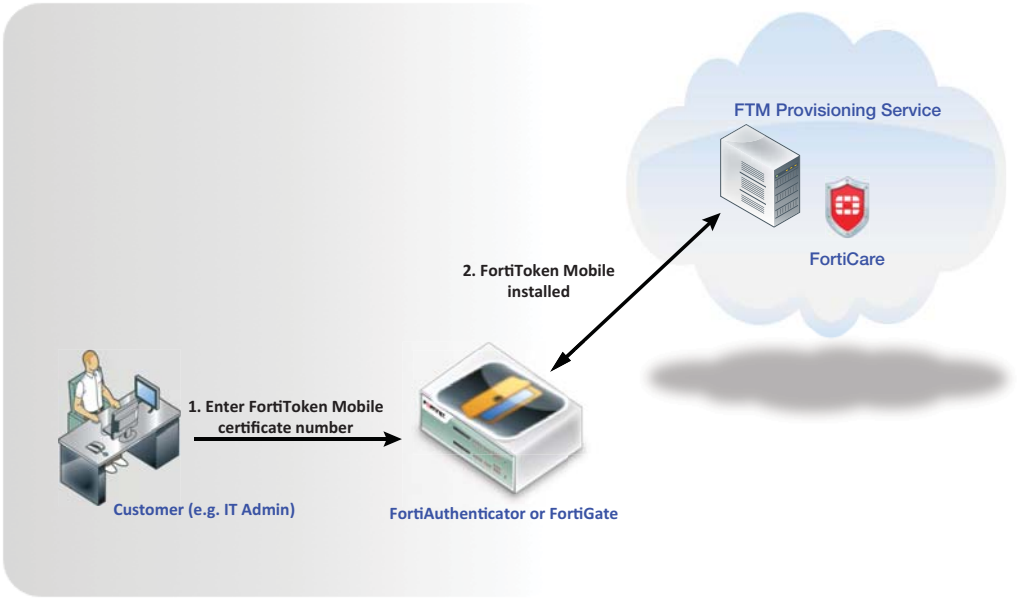
Installing FortiToken Mobile tokens

You will need a certificate code to install FortiToken Mobile tokens. There are two options for getting FortiToken Mobile token certificate codes for use on your authentication server; FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

The FortiToken Mobile installation process is the same for the Redemption Certificate and the Free Trial Tokens.

1. The authentication server administrator enters the certificate code.
2. The authentication server sends code to FortiToken Mobile provisioning server serial numbers, which validates the request, registers the FortiToken Mobile license and sends the FortiToken Mobile serial numbers back to the authentication server.

Figure 1: FortiToken Mobile installation context



Redemption certificate

For each FortiToken Mobile purchase, you will receive a redemption certificate for the number of tokens purchased. The activation code is 20 digits, revealed by scratching off the designated area of the certificate.

Figure 2: Sample redemption certificate for 200 FortiToken Mobile tokens

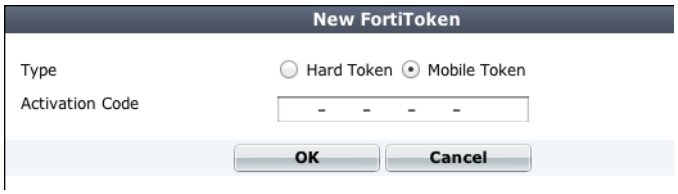
"Virtual" certificate for free trial tokens

Each FortiGate or FortiAuthenticator device comes with a trial license for two free trial tokens. The device must be registered with FortiCare to retrieve the tokens. The certificate code to use for the free trial FTM tokens is 0000-0000-0000-0000-0000.

FortiToken Mobile installation

To install the token on a FortiGate unit

1. Located the 20 digit code on the redemption certificate.
2. Login to the FortiGate Web-based manager.
3. Go to *User & Device* > *Two-factor Authentication* > *FortiToken* and select *Create New*.
4. Select *Mobile Token.*

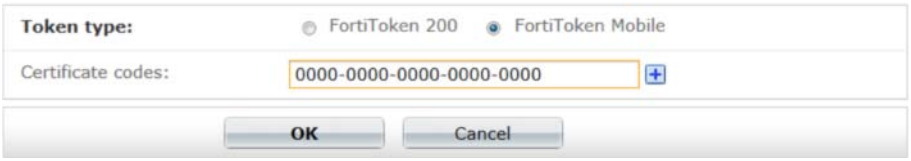


5. Enter the 20 digit certificate code in the *Activation Code* box.
6. Select *OK*.

Figure 3: Token list in FortiOS

To install the token on a FortiAuthenticator unit

1. Locate the 20 digit code on the redemption certificate.
2. Login to the FortiAuthenticator Web-based manager.
3. Go to Authentication > *Local User Management* > *FortiTokens*.
4. Select *Create New* and select *Mobile Token*.



5. Enter the 20 digit certificate code in the *Activation Code* box
6. Select *OK*.

Figure 4: Token list in FortiAuthenticator

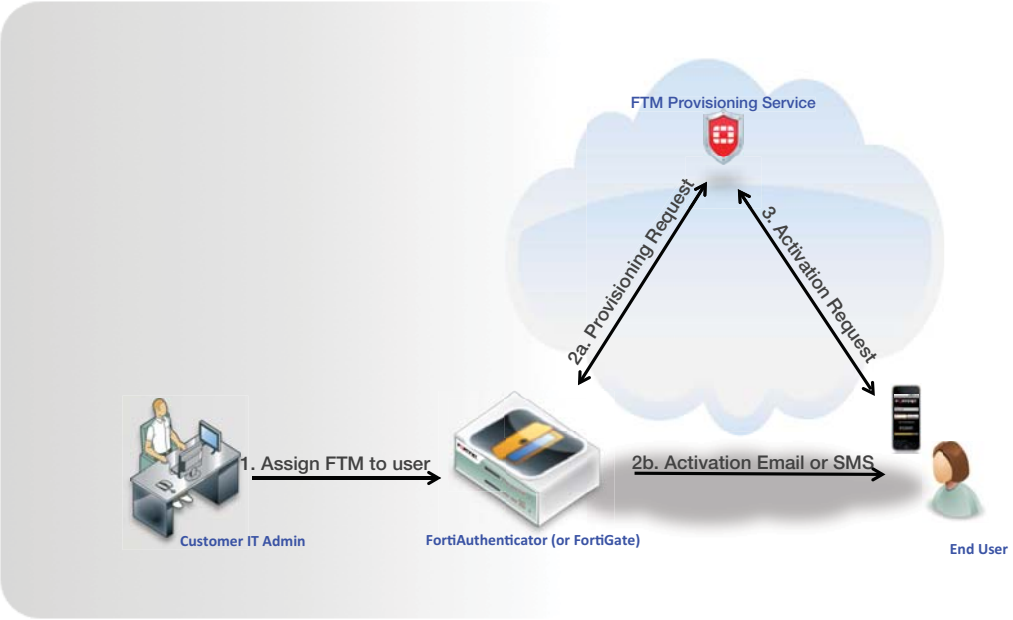
Provisioning and activating FortiToken Mobile tokens

The FTM provisioning and activation operations include:

1. Authentication Server administrator has to first assign a FortiToken Mobile token to the user.
2. **a.** The Authentication Server notifies the Provisioning Server that the token has been assigned for subsequent activation and receives back an activation code to forward to the end user

   b. The end user receives an activation notification via email or SMS, depending on how the Authentication Server is configured.
3. After installing the FortiToken Mobile app on the mobile device, the end-user can activate the token anytime within a configurable provisioning time period.

Figure 5: Activating tokens

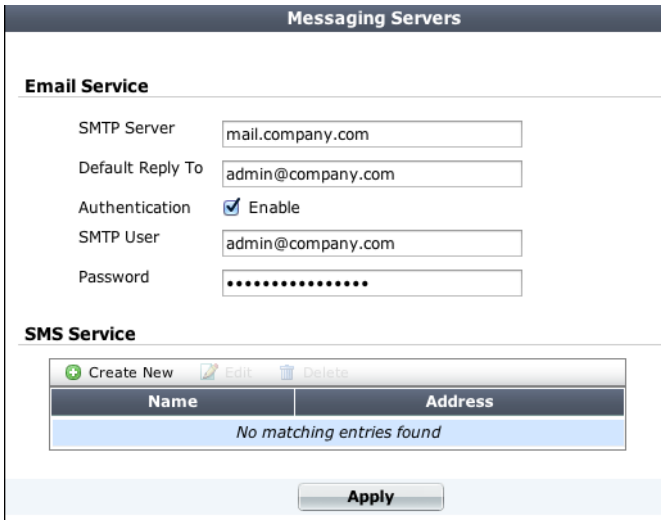


FortiToken Mobile provisioning on a FortiGate unit

To ensure messaging functions properly, configure the messaging servers, and configure users to receive messages from the server and use the FortiToken Mobile token.

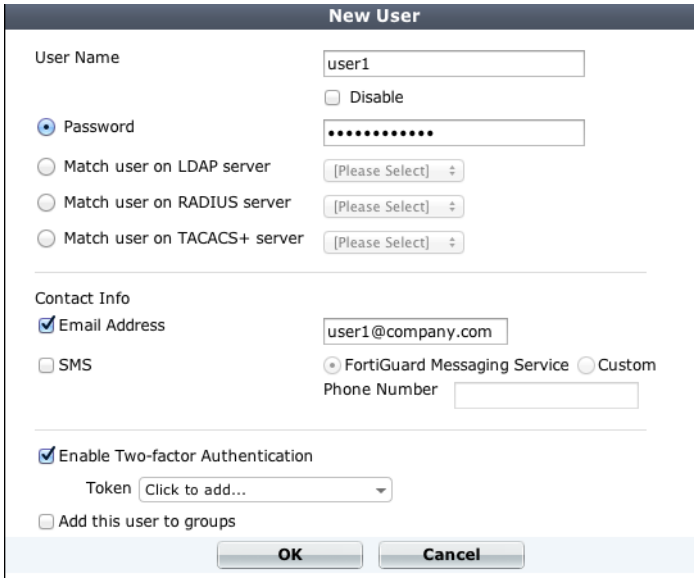
To setup FortiToken Mobile provisioning

1. Go to *System* > *Config* > *Messaging Servers*.
2. Configure the servers as required.



3. Go to *User & Device* > *User* > *User Definition*.

4. Select the user, or select *Create New*.



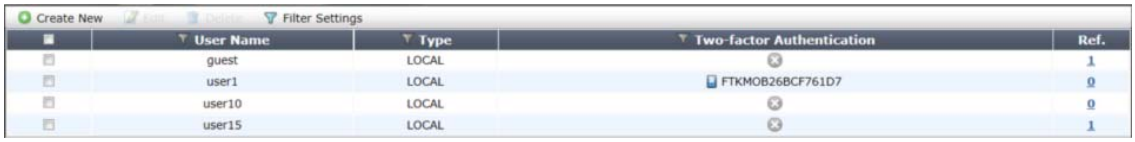
5. In *Contact Info*, select either the email address or phone number for SMS messages.
6. Select *Enable Two-factor Authentication* and select an available token.
7. Select *OK*.

The activation code will expire after a configurable period of time. To configure the time period, use the CLI command:

```
config system global
   set two-factor-ftm-expir <time-in-hours>
end
```

Note: The two-factor-ftm-expiry value should be in the range of 1-168.

Figure 6: Token assignment list



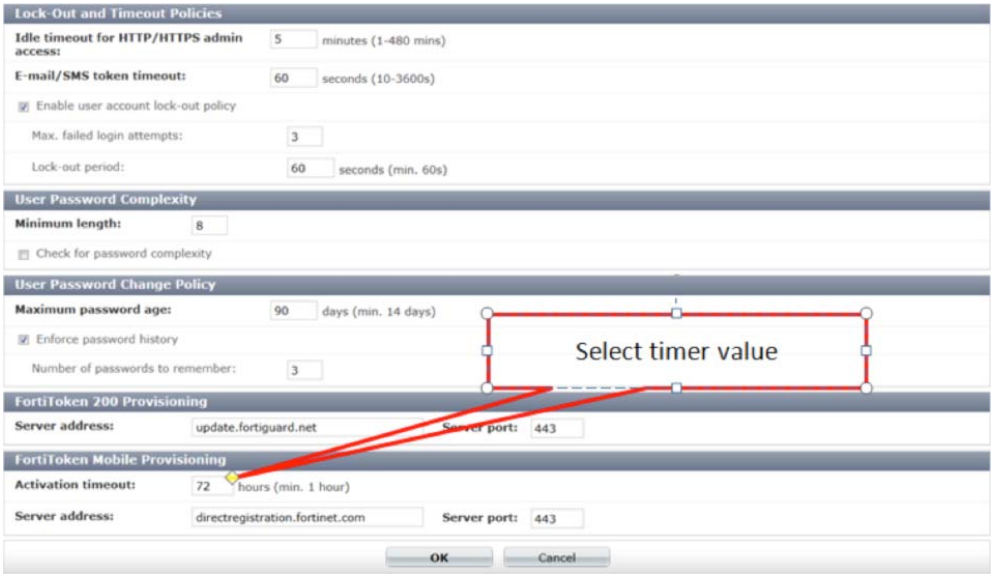
FortiToken Mobile provisioning on a FortiAuthenticator unit

To ensure messaging functions properly, configure the messaging servers, and configure users to receive messages from the server and use the FortiToken Mobile token.

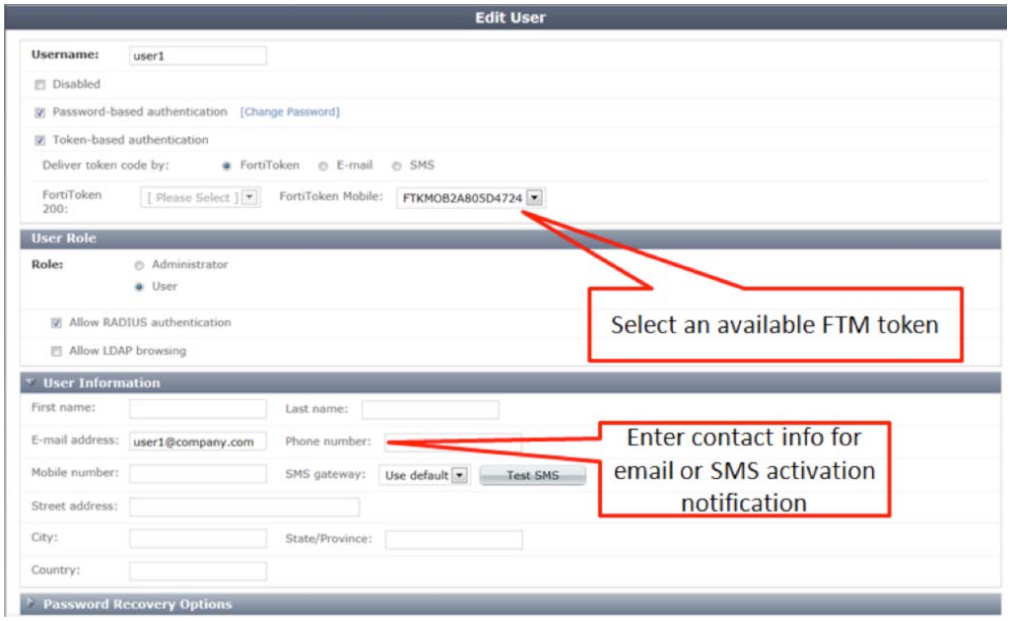
To setup FortiToken Mobile provisioning

1. Go to *System* > *Messages* > *SMTP Servers*, or *System* > *Messages* > *SMS Gateways*.
2. Configure the servers as required.

3. Got to *Authentication* > *General* > *Options* and ensure the interval time period is set. The interval is the time period in hours in which the end user must activate the token before having to re-provision the token.



4. Go to *Authentication* > *Local User Management* > *Local* or *Authentication* > *Local User Management* > *Remote.*
5. Select a user or select *Create New*.



6. In *User Information*, select either the email address or phone number for SMS messages.
7. Select select an available FortiToken Mobile token.
8. Select *OK*.

Figure 7: Token assignment list

FortiToken Mobile client activation

After successfully assigning a token to the end user, the end user will receive an activation notification as seen in the example below for email notification:

```
Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit
http://docs.fortinet.com/auth/FortiToken-Mobile-User-Guide-10.pdf

for instructions on how to install your FortiToken Mobile application
on your device and activate your token.

Your Activation Code, which you will need to enter on your device later,
is “F9E801EB”. You must activate your token by: Mon Oct 15 23:47:04 2012
GMT+00:00, after which you will need to contact your system
administrator to re-enable your activation.
```

The end user must enter the 8 character activation code into the FortiToken Mobile app within the activation window given in the notification.

Figure 8: Activating the token

This will trigger an activation request to the provisioning server. If the request is valid, the FortiToken Mobile will be activated and ready to use on the mobile device.

FortiToken Mobile token status

The meanings of the three possible status values for FortiToken Mobile tokens are:

- Available: FortiToken Mobile token is available for provisioning
- Pending: FortiToken Mobile token is provisioned but not yet activated
- Assigned: FortiToken Mobile token is activated
- Locked: FortiToken Mobile tokens will be locked automatically if an Assigned token is Un-assigned when FortiCare FortiToken Mobile Provisioning Server is unreachable.
  - To unlock the locked token in FOS when FortiToken Mobile Provisioning Server is reachable, use the following CLI command:

    ```
    execute fortitoken-mobile renew <ftm-sn>
    ```

  - To unlock the locked token in FortiAuthenticator, use the unlock button on the FortiToken user interface.

Figure 9: FortiToken Mobile Provisioning Status in FortiOS

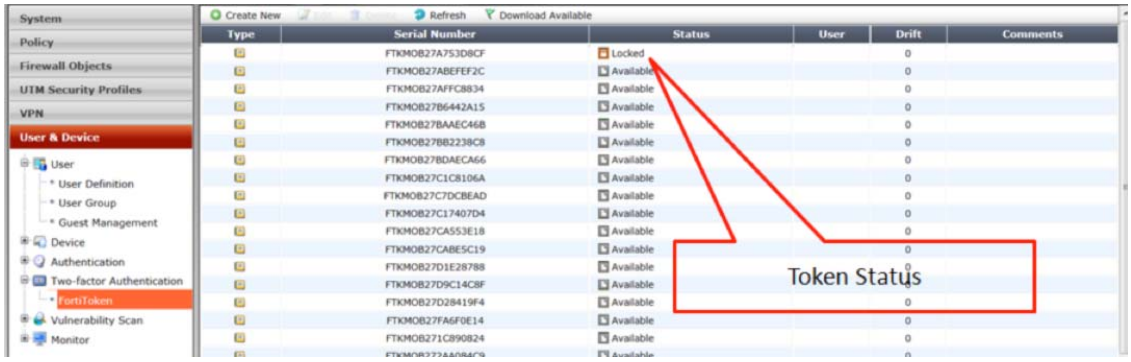


Figure 10: FortiToken Mobile Provisioning Status in FortiAuthenticator